Minimum-cost quantum measurements for quantum information

Minimum-cost quantum measurements for quantum information

Petros Wallden,[1, 2, *] Vedran Dunjko,[3, 1, 4, 5] and Erika Andersson[1]

[1] *SUPA, Institute of Photonics and Quantum Sciences, School of Engineering and Physical Sciences, Heriot-Watt University, Edinburgh EH14 1AS, UK*
[2] *Physics Department, University of Athens, Panepistimiopolis 157-71, Ilisia Athens, Greece*
[3] *Now at: Institute for Quantum Optics and Quantum Information, Austrian Academy of Sciences, Technikerstr. 21A, A-6020 Innsbruck, Austria*
[4] *School of Informatics, Informatics Forum, University of Edinburgh, 10 Crichton Street, Edinburgh EH8 9AB, UK.*
[5] *Laboratory of Evolutionary Genetics, Division of Molecular Biology, Ruđer Bošković Institute, Bijenička cesta 54, 10000 Zagreb, Croatia*

Knowing about optimal quantum measurements is important for many applications in quantum information and quantum communication. However, deriving optimal quantum measurements is often difficult. We present a collection of results for minimum-cost quantum measurements, and give examples of how they can be used. Among other results, we show that a minimum-cost measurement for a set of given pure states is formally equivalent to a minimum-error measurement for mixed states of those same pure states. For pure symmetric states it turns out that for a certain class of cost matrices, the minimum-cost measurement is the square-root measurement. That is, the optimal minimum-cost measurement is in this case the same as the minimum-error measurement. Finally, we consider sequences of individual "local" systems, and examine when the global minimum-cost measurement is a sequence of optimal local measurements. We also a consider an example where the global minimum-cost measurement is, perhaps counter-intuitively, not a sequence of local measurements, and discuss how this is related to related to the Pusey-Barrett-Rudolph argument for the nature of the wave function.

I. INTRODUCTION

The problem of finding optimal quantum measurements which decode classical information stored in quantum states, with various optimization criteria, has been studied since the very beginnings of quantum information theory [1]. A common scenario is minimum-error measurements. Here, given a known ensemble of quantum states $\{\rho_i, \eta_i\}_i$, where η_i is the probability with which the state ρ_i appears, the task is to find a measurement which minimizes the average error probability in the result. Somewhat more generally, different types of error in the result can carry different costs according to a so-called cost matrix. The measurement which minimizes the average cost is then called the minimum-cost measurement. In a quantum communication situation, classical information i could first be encoded into a quantum state ρ_i, after which one may want to decode it back to classical information via a quantum measurement. For example, finding relevant optimal figures of merit often plays an important role in security proofs of quantum cryptographic protocols, where an adversary tries to obtain information about a quantum state. Optimal so-called generalised quantum measurements are certainly not only of theoretical interest, but have also been experimentally realized on photons, see for example [2], on NV centres [3], and could be realized on trapped ions or atoms with existing experimental means [4].

Finding optimal quantum measurements is in general hard. Optimal strategies have been obtained for some special cases, with various assumptions on the initial states. For minimum-error measurements, for instance, the input states usually have to possess some kind of symmetry [1, 5–8]. An exception is the minimum-error measurement for arbitrary pure qubit states, occurring with uniform probability, which was obtained by Hunter [9]. A general geometric structure of the minimum-error problem was given only recently [10]. Minimum-cost settings have been much less studied [1, 11].

In this paper, we study both minimum-error and minimum-cost measurements, and establish a link between minimum-cost measurements for pure states and minimum-error measurements for mixed states. We then apply the general results we obtain to symmetric states, and their natural generalization, states which are sequences of (that is, tensor products of) symmetric states. Symmetric states are ubiquitous in quantum information. Quantum key distribution (QKD) using the BB84 protocol [12] or coherent states [13, 14], universal blind quantum computing (UBQC) [15] and quantum digital signatures (QDS) [16–19], for instance, use trains of independent symmetric states,

*Electronic address: petros.wallden@hw.ac.uk

giving rise to a tensor product structure. Optimal measurements on whole trains of states, versus measurements on individual elements, are analogous to individual and collective/coherent attacks in QKD.

The outline of this paper is as follows. We begin by proving some general results concerning minimum-cost measurements, and establish a formal equivalence between minimum-cost measurements for pure states and minimum-error measurements for mixed states. Following this, we focus on the minimum-cost problem of the so-called symmetric states, for both mixed and pure states. Finally, we explore the minimum-cost problem for states which are tensor products of individual (local) states, motivated by situations which often appear in quantum cryptographic protocols. We analyse when the local measurements are the minimum-cost, give example that the minimum-cost measurement is global and highlight a connection with the Pusey, Barrett and Rudolph (PBR) argument for the nature of the wave function [20] and quantum state elimination measurements [21, 22]. We conclude with a brief discussion.

II. GENERAL RESULTS FOR MINIMUM-COST MEASUREMENTS

Suppose that some quantum states ρ_i each occur with probability η_i, and that we are making a quantum measurement described by the measurement operators Π_j. We will denote the measurement by Π, and also define $B_{i,j}(\Pi) = Tr(\Pi_j \rho_i)$ as the probability to obtain result j given that the state was ρ_i. Because probabilities have to be positive, it follows that the operators Π_i have to be positive semi-definite. Also, since probabilities for all possible outcomes (including not obtaining a result, if this may happen) should sum to one, it holds that $\sum_i \Pi_i = \mathbb{I}$.

Further, suppose that obtaining result j when the state was ρ_i carries a cost $C_{i,j}$. The average cost of the measurement $\Pi = \{\Pi_k\}_k$, with respect to the (real) cost matrix $C = [C_{i,j}]$ is denoted $\bar{C}(\Pi)$ and is given by

$$\bar{C}(\Pi) = \sum_{i,j} \eta_i C_{i,j} Tr(\Pi_j \rho_i). \tag{1}$$

The minimum cost is obtained by minimizing this average cost over all possible POVM's $\{\Pi_i\}$,

$$\bar{C}_{min} = \min_{\{\Pi\}} \bar{C}(\Pi). \tag{2}$$

It is well established [1] that a minimum-cost measurement is optimal if and only if the following criteria are met:

1. $\Gamma = \sum_j \Pi_j W_j = \sum_j W_j \Pi_j$ for $W_j = \sum_i \eta_i C_{i,j} \rho_i$.
2. $\Gamma = \Gamma^\dagger$.
3. $\Pi_j (W_j - \Gamma) = (W_j - \Gamma)\Pi_j = 0$ for all j.
4. $(W_j - \Gamma)$ is positive semidefinite for all j.

It can be shown that the three first conditions are equivalent to

$$\Pi_i (W_i - W_j) \Pi_j = 0. \tag{3}$$

This form of the conditions was first derived by Holevo [23] and Yuen et al. [24] independently. We will refer to the criteria above, as is usually done, as the Helstrom criteria.

For minimum-cost measurements we can prove the following general properties, which we first give informally. Keeping the states ρ_i and prior probabilities η_i the same,

1. The optimal measurement remains the same if the same column is added to or subtracted from each of the columns of the cost matrix. This means that the costs associated with different outcomes, for the same prior state ρ_i, all shift by the same amount. The average cost will also shift by a fixed amount.
2. The average minimal cost is superadditive with respect to the cost matrix. This means that the sum of the optimal minimal costs for some cost matrices $C^1, \ldots, C^n$ is lower than the minimal cost for the cost matrix $\sum_{k=1}^n C^k$.
3. Increasing (decreasing) each entry of the cost matrix by a varying amount increases (decreases) the optimal minimum cost of the problem. In other words, the minimum cost is monotone under the point-wise partial order of the cost matrices.

A special class of minimum-cost problems is the well-studied minimum-error problem. In the minimum-error problem the task is to, given some fixed set of states with some prior probabilities, find the measurement (and the ensuing success probability) which, on average, minimizes the probability of an error in the result. It is easy to see that this is a special class of minimum-cost problems, for a cost matrix with elements $C_{i,j} = A - \delta_{i,j}$ for any (real) constant A. If we choose $A = 1$, then the minimum cost $\bar{C}_{min}$ is the minimum-error probability. At the end of this section, we will show that there is an additional one-to-one correspondence between minimum-error measurements on mixed states and minimum-cost measurements for pure states.

Next, we will formally state and prove the above claims for minimum-cost measurements. In this paper, whenever there is addition or subtraction in matrix indices, this is understood as modular addition or subtraction. For example, if A is an $N \times M$ matrix, then $A_{i+N,j+M} = A_{i,j}$.

Lemma 1 *Assume a minimum-cost problem with the cost matrix with elements $C_{i,j}$, where the states ρ_i appear with the frequencies η_i. If we add (subtract) a* constant-row cost matrix *with elements $C^r_{i,j} = C^r_i$, to (from) the original cost matrix, i.e. $C^t_{i,j} = C_{i,j} \pm C^r_{i,j}$, then the following two properties hold.*

(a) The measurement that gives the minimum cost for the problem with the cost matrix $C^t_{i,j}$ also gives the minimum cost for $C_{i,j}$. That is, the measurement that gives the minimum cost is not altered.

(b) The minimum cost of C^t is equal to the minimum cost of C, shifted by the cost of the constant row matrix $\bar{C}^r = \sum_i \eta_i C^r_i$.

Proof:
First note that a cost matrix with fixed elements in each row (a *constant-row matrix*), i.e. $C_{i,j} = C_{i,j+k} = c_i \forall k$, gives the same cost for *every* measurement, and this cost is equal to $\bar{C}^r = \sum_i \eta_i c_i$. This follows from

$$\bar{C}^r(\Pi) = \sum_{i,j} \eta_i C^r_{i,j} Tr(\Pi_j \rho_i) = \sum_i \eta_i c_i Tr((\sum_j \Pi_j)\rho_i) = \sum_i \eta_i c_i = \bar{C}^r. \tag{4}$$

Therefore, all measurements are optimal for such a minimum-cost problem. For the situation in this lemma, the total cost is given by

$$\begin{aligned} \bar{C}^t(\Pi) &= \sum_{i,j} \eta_i (C_{i,j} \pm C^r_{i,j}) Tr(\Pi_j \rho_i) = \sum_{i,j} \eta_i C_{i,j} Tr(\Pi_j \rho_i) \pm \sum_i \eta_i c_i \\ &= \bar{C}(\Pi) \pm \sum_i \eta_i c_i = \bar{C}(\Pi) \pm \bar{C}^r. \end{aligned} \tag{5}$$

Now it is easy to see that our lemma holds as the second (additive) term on the rightmost side of the equation above is independent of the measurement Π. Thus the changed cost matrix $C^t_{i,j}$ yields the same optimal measurement, with the minimum shifted by $\sum_i \eta_i c_i = \bar{C}^r$. ■

Lemma 2 *Let C be a cost matrix such that $C_{i,j} = \sum_k C^k_{i,j}$, for some individual cost matrices $C^k, k = 1, \ldots n$. Then the minimum cost induced by the cost matrix C is bounded from below by the sum of the individual minimum costs induced by the individual cost matrices appearing in the sum, i.e. $\bar{C}_{min} \geq \sum_k \bar{C}^k_{min}$.*

Proof:
For any measurement Π it holds that

$$\bar{C}(\Pi) = \sum_k \bar{C}^k(\Pi). \tag{6}$$

Suppose that the measurement Π' gives the minimum cost for the total cost matrix, and that the measurements Π^k give the minimum costs for the cost matrices C^k, respectively. We then have

$$\bar{C}_{min} = \bar{C}(\Pi') = \sum_k \bar{C}^k(\Pi') \geq \sum_k \bar{C}^k(\Pi^k) = \sum_k \bar{C}^k_{min}. \tag{7}$$

■

Lemma 3 *Assume that we have a cost matrix $C = [C_{i,j}]$, and an element-wise smaller cost matrix $C^l = [C^l_{i,j}]$, with $C^l_{i,j} \leq C_{i,j}$ for all i, j, and an element-wise larger cost matrix $C^u = [C^u_{i,j}]$ with $C^u_{i,j} \geq C_{i,j}$ for all i, j. Then the minimum cost induced by the cost matrix C is bounded from below by the minimum cost induced by C^l and from above by the minimum cost of C^u. In other words,*

$$\bar{C}^l_{min} \leq \bar{C}_{min} \leq \bar{C}^u_{min}. \tag{8}$$

Proof:
We can write $C_{i,j} = C^l_{i,j} + C^s_{i,j}$, where C^s is a strictly positive cost matrix. If the cost matrix has only non-negative real elements then for any measurement Π we have that $\bar{C}^s(\Pi) \geq 0$. From Lemma 2 it follows that

$$\bar{C}_{min} = \min_{\Pi} \bar{C}(\Pi) \geq \min_{\Pi} \bar{C}^l(\Pi) + \min_{\Pi} \bar{C}^s(\Pi) \geq \min_{\Pi} \bar{C}^l(\Pi) = \bar{C}^l_{min} \tag{9}$$

Similarly, by noting that $C_{i,j} + C^s_{i,j} = C^u_{i,j}$ for some positive cost matrix C^s we conclude that $\bar{C}_{min} \leq \bar{C}^u_{min}$. ■

We will use these lemmas in the remainder of this paper.

III. MINIMUM-ERROR MEASUREMENTS OF MIXED STATES AS MINIMUM-COST MEASUREMENTS OF PURE STATES

Here we point out an equivalence between minimum-error measurements for mixed states and minimum-cost measurements for pure states. Using the results in this subsection, we will then in the next section provide analytic bounds on the minimum-error probabilities of a wide class of mixed states, and also, for some special cases, give analytical expressions for the minimum-error probability.

As we have noted, a minimum-error measurement is simply a minimum-cost measurement for distinguishing between the same set of states, with a cost matrix given by $C_{i,j} = 1 - \delta_{i,j}$. Suppose that we are interested in the minimum-error problem where the input states are a collection of N mixed states $\{\rho_i\}$, appearing with respective frequencies $\{\eta_i\}_i$, of the form

$$\rho_i = \sum_m a_{i,m} \left|\psi_m\right\rangle \left\langle\psi_m\right|, \tag{10}$$

where $a_{i,m}$ are $N \times N$ coefficients such that $\sum_m a_{i,m} = 1$, and $\{\left|\psi_1\right\rangle, \cdots, \left|\psi_N\right\rangle\}$ are N pure states. Then, the minimum-error measurement minimizes the expression

$$P_{err}(\Pi) = C(\Pi) = \sum_{i,j} \eta_i (1 - \delta_{i,j}) Tr(\Pi_j \rho_i) = 1 - \sum_i \eta_i Tr(\Pi_i \rho_i). \tag{11}$$

This minimum-error problem for the N mixed states in (10), occurring with prior probabilities η_i, is equivalent to a minimum-cost problem for the N equiprobable pure states $\{\left|\psi_j\right\rangle\}_j$, with the cost matrix

$$C_{m,i} = 1 - N \eta_i a_{i,m} \tag{12}$$

(note the inverse order of indices in $C_{m,i}$). This can be seen from the following derivation,

$$\begin{aligned} P_{err}(\Pi) &= 1 - \sum_i \eta_i Tr(\Pi_i \rho_i) = 1 - \sum_i \eta_i Tr(\Pi_i \sum_m a_{i,m} \left|\psi_m\right\rangle \left\langle\psi_m\right|) \\ &= 1/N \left(\sum_{i,m} Tr(\Pi_i \left|\psi_m\right\rangle \left\langle\psi_m\right|) - \sum_{i,m} N \eta_i a_{i,m} Tr(\Pi_i \left|\psi_m\right\rangle \left\langle\psi_m\right|) \right) \\ &= 1/N \sum_{i,m} C_{m,i} Tr(\Pi_i \left|\psi_m\right\rangle \left\langle\psi_m\right|) = C(\Pi), \end{aligned} \tag{13}$$

where $C(\Pi)$ is the cost of the measurement corresponding to the POVM $\{\Pi\}$ for the pure states $\{\left|\psi_m\right\rangle\}$ with equal prior probabilities $1/N$ and cost $C_{m,i}$ that is defined in Eq. (12). This shows that for *any* measurement (POVM) $\{\Pi\}$, the cost for the considered pure states is the same as the error probability for the mixed states. It follows that the minimum-cost measurement for the pure states will also be the minimum-error measurement for the mixed states, with prior probabilities as stated above. Another thing to note regarding Eq. (12) is that in the case where $a_{i,j} = \delta_{i,j}$, it reduces to the usual formula for a minimum-error measurement on pure states.

IV. MINIMUM-COST MEASUREMENTS FOR PURE SYMMETRIC STATES

In this section we will consider minimum-cost measurements for pure symmetric states. In the section following this one, we will use these results to obtain the minimum-error probability for certain classes of mixed states, in particular, for mixed states that are mixtures of pure symmetric states. We will first consider the Square Root Measurement (SRM), which is known to be the minimum-error measurement for pure symmetric states. We will express the success probability of the SRM (that is, the minimum-error measurement) as a function of the eigenvalues of the Gram matrix of the states we are considering. Following this, we will extend the minimum-error problem to a minimum-cost problem and prove that for certain class of cost matrices, the SRM is the minimum-cost measurement. We will then apply the results of the previous sections to provide bounds for the minimum cost in an example, for four symmetric coherent states with equal amplitude but different phases.

Let U be a unitary such that $U^N = I$. We define $|\psi_i\rangle = U^i |\psi_0\rangle$ for some $|\psi_0\rangle$. The N states $\{|\psi_0\rangle, \cdots, |\psi_{N-1}\rangle\}$ are called *symmetric*, and we will call U the *symmetry unitary*. We furthermore assume that the prior probabilities for the states are equal i.e. $\eta_i = 1/N$. We define

$$B_{i,j} = Tr(\Pi_j \rho_i) = \langle\psi_i| \Pi_j |\psi_i\rangle , \tag{14}$$

which is the probability that outcome j is obtained, using the measurement $\{\Pi\}$, if the state sent was ρ_i. We can then rewrite the cost as

$$\bar{C}(\Pi) = 1/N \sum_{i,j} B_{i,j} C_{i,j} \tag{15}$$

where we have used $\eta_i = 1/N$.

A. SRM measurement of symmetric states

The square root measurement is known to be the minimum-error measurement for many cases, such as for pure symmetric states [1], for pure multiply symmetric states [6] and for a certain class of mixed states [8] where at least one state has strictly positive coefficients when written in the symmetry operator eigenbasis. In the present paper, we will show that this measurement is important for a much wider range of cases, involving minimum-cost measurements and minimum-error measurements for certain mixed states (exact conditions will be given later). We will also show how it is possible to bound the minimum cost and minimum-error probabilities for even more cases. If we define

$$\Phi = \sum_{i=0}^{N-1} |\psi_i\rangle \langle\psi_i| , \tag{16}$$

then the square root measurement is defined by

$$\Pi_j = \Phi^{-1/2} |\psi_j\rangle \langle\psi_j| \Phi^{-1/2} = |\phi_j\rangle \langle\phi_j| \tag{17}$$

where

$$|\phi_j\rangle = \Phi^{-1/2} |\psi_j\rangle . \tag{18}$$

The Gram matrix of the states we are trying to distinguish between is defined as

$$G_{i,j} := [\langle\psi_i|\psi_j\rangle]_{i,j} = \left[\langle\psi_0| (U^i)^\dagger U^j |\psi_0\rangle\right]_{i,j} = \left[\langle\psi_0| U^{j-i} |\psi_0\rangle\right]_{i,j} , \tag{19}$$

since $(U^i)^\dagger$ is the unique inverse of U^i, and therefore $(U^i)^\dagger = U^{N-i} = U^{-i}$. A matrix is circulant if $A_{i,j} = A_{i+k,j+k}$ where the addition is taken modulo N. The Gram matrix of the symmetric states is circulant, since it depends only on the difference $(j - i)$.

We should also note that we can write U as

$$U = \sum_{k=0}^{D-1} \exp(2\pi I k/N) |\gamma_k\rangle \langle\gamma_k| , \tag{20}$$

where $\{|\gamma_k\rangle\}_D$ is an orthonormal basis and D is the dimension of the space spanned by the $|\psi_i\rangle$. We therefore have $\langle\gamma_k|\gamma_{k'}\rangle = \delta_{k,k'}$. Note, that in general $N \neq D$, and it is important to keep track of in what range each index is defined.

For the special case of linearly independent symmetric states, $N = D$ and the derivations simplify. By expressing $|\psi_0\rangle$ in terms of $|\gamma_k\rangle$,

$$|\psi_0\rangle = \sum_{k=0}^{D-1} b_k \, |\gamma_k\rangle \, , \tag{21}$$

we obtain

$$|\psi_i\rangle = \sum_{k=0}^{D-1} b_k \exp(2\pi I i k/N) \, |\gamma_k\rangle \, . \tag{22}$$

We can then express the Gram matrix G which is $N \times N$ matrix, in terms of a matrix M which is $D \times N$ matrix,

$$G = M^\dagger M, \tag{23}$$

where

$$M = \begin{pmatrix} \langle\gamma_0|\,\psi_0\rangle, & \langle\gamma_0|\,\psi_1\rangle, & \cdots, & \langle\gamma_0|\,\psi_{N-1}\rangle \\ \langle\gamma_1|\,\psi_0\rangle, & \langle\gamma_1|\,\psi_1\rangle, & \cdots, & \langle\gamma_1|\,\psi_{N-1}\rangle \\ \cdots, & \cdots, & \cdots, & \cdots \\ \langle\gamma_{D-1}|\,\psi_0\rangle, & \langle\gamma_{D-1}|\,\psi_1\rangle, & \cdots, & \langle\gamma_{D-1}|\,\psi_{D-1}\rangle \end{pmatrix}. \tag{24}$$

The columns of M are representations of the $|\psi_i\rangle$'s in the $|\gamma_k\rangle$ basis. We have

$$[M]_{i,j} = \langle\gamma_i|\,\psi_j\rangle = b_i \exp(2\pi I i j/N). \tag{25}$$

The Gram matrix, being circulant, can be diagonalised with the unitary discrete fourier transform F,

$$F_{i,j} = 1/\sqrt{N} \exp(-2\pi I i j/N), \tag{26}$$

and therefore

$$F^\dagger G F = F^\dagger M^\dagger M F = (MF)^\dagger MF = \Lambda, \tag{27}$$

where Λ is a diagonal matrix with the eigenvalues λ_k of G on the diagonal. With the above definitions we can see that

$$\begin{aligned} [MF]_{i,k} &= \sum_j [M]_{i,j}[F]_{j,k} = \sum_j b_i \exp(2\pi I i j/N) 1/\sqrt{N} \exp(-2\pi I j k/N) \\ &= b_i \delta_{i,k} \sqrt{N}, \end{aligned} \tag{28}$$

which leads to

$$\begin{aligned} \lambda_i &= N|b_i|^2 \text{ for } i < D \\ \lambda_i &= 0 \text{ otherwise.} \end{aligned} \tag{29}$$

In the derivation above we used the fact that $\sum_j [\exp(2\pi I(i-k)j/N)] = N\delta_{i,k}$. We can now rewrite the initial states $|\psi_i\rangle$ in terms of the eigenvalues of the Gram matrix,

$$|\psi_i\rangle = 1/\sqrt{N} \sum_{k=0}^{D-1} \sqrt{\lambda_k} \exp(2\pi I i k/N) \, |\gamma_k\rangle \, . \tag{30}$$

In the basis of the $|\gamma_k\rangle$, the average operator Φ in Eq. (16) becomes

$$\begin{aligned} \Phi &= 1/N \sum_{k=0}^{N-1} \sum_{i,j=0}^{D-1} \sqrt{\lambda_i \lambda_j} \exp(2\pi I i k/N) \exp(-2\pi I j k/N) \, |\gamma_i\rangle \, \langle\gamma_j| \\ &= 1/N \sum_{k=0}^{N-1} \sum_{i,j=0}^{D-1} \sqrt{\lambda_i \lambda_j} \exp(2\pi I (i-j) k/N) \, |\gamma_i\rangle \, \langle\gamma_j| \\ &= \sum_{i=0}^{D-1} \lambda_i \, |\gamma_i\rangle \, \langle\gamma_i| \, , \end{aligned} \tag{31}$$

where we in the last step used the fact that λ_i are all non-negative. In this basis, the average operator is thus diagonal and the elements on the diagonal are the first D eigenvalues of the Gram matrix. Since the first D eigenvalue are non-zero (are related with the D-coefficients b_i from eq. (29), which can be taken to be non-zero), the inverse in this basis is diagonal with elements $1/\lambda_i$. Therefore Eq. (18) becomes

$$|\phi_i\rangle = \Phi^{-1/2}|\psi_i\rangle = 1/\sqrt{N}\sum_{k=0}^{D-1}\exp(2\pi Iik/N)|\gamma_k\rangle\,, \tag{32}$$

which are the DFT transformed $|\gamma_k\rangle$'s. We now obtain

$$B_{i,j} = |\langle\psi_i|\phi_j\rangle|^2 = (1/N^2)|\sum_{k=0}^{D-1}\sqrt{\lambda_k}\exp(2\pi I(j-i)k/N)|^2. \tag{33}$$

It is worth mentioning that the operator B with the matrix elements $B_{i,j}$ is both circulant and symmetric.

The cost of making the SRM, for a cost matrix $C_{i,j}$, is given by

$$\bar{C}_{SRM} = \sum_{i,j=0}^{N-1}\eta_i B_{i,j}C_{i,j}. \tag{34}$$

We will see later that under certain circumstances this is also the minimum cost. For now, let us assume that the prior probabilities are equal, $\eta_i = 1/N$, and that the cost matrix is circulant, i.e. that the matrix elements obey $C_{i,i+k} = C_{j,j+k} = \sum_k c_k\delta_{k,j-i}$. We then obtain

$$\bar{C}_{SRM} = 1/N^2\sum_{k=0}^{N-1}c_k|\sum_{l=0}^{D-1}\sqrt{\lambda_l}\exp(2\pi Ikl/N)|^2. \tag{35}$$

The minimum-error probability, which is the cost for $C_{i,j} = 1-\delta_{i,j}$, i.e. $c_k = 1-\delta_{k,0}$, becomes

$$p_{min} = 1-(1/N^2)|\sum_{i=0}^{D-1}\sqrt{\lambda_i}|^2. \tag{36}$$

B. When is the SRM the minimum-cost measurement?

In this section we will investigate under what conditions the minimum-cost measurement for N symmetric states is the SRM, with a minimum cost given by Eq. (35). In particular, we will examine the Helstrom conditions separately, and see what sufficient conditions we can impose on the cost matrix, such that the SRM is the optimal minimum-cost measurement. For circulant and symmetric cost matrices, the three first Helstrom conditions are satisfied by the SRM, as shown in supplementary material of [17]. Here we will give an easier way to prove those conditions. We will then show that if the cost matrix obeys one more condition, then the last Helstrom condition, the inequality, also holds for the SRM, and thus the minimum-cost measurement for this type of cost matrices is the SRM.

Theorem 1 *Let $\rho_i = |\psi_i\rangle\langle\psi_i|$ be N symmetric pure states, with equal prior probabilities $\eta_i = 1/N$, and let $C_{i,j}$ be an $N\times N$ cost matrix which is circulant and symmetric. The three first Helstrom conditions for minimum-cost measurements can be re-written as the three first Helstrom conditions for a minimum-error measurement of the modified states $\rho'_i := \sum_j C_{i,j}\rho_j$. That is,*

$$\Pi_i(\rho'_i - \rho'_j)\Pi_j = 0 \tag{37}$$

for all i,j. This condition holds for $\Pi_i = |\phi_i\rangle\langle\phi_i|$,which is the SRM for the initially considered pure states.

Proof:
Eq. (37) becomes

$$\sum_{k=0}^{N-1}C_{i,k}\langle\phi_i|\psi_k\rangle\langle\psi_k|\phi_j\rangle - \sum_{l=0}^{N-1}C_{j,l}\langle\phi_i|\psi_l\rangle\langle\psi_l|\phi_j\rangle = 0 \tag{38}$$

We can find, for every term in the first sum, a corresponding term in the second sum, so that these terms cancel. The elements of the cost matrix $C_{i,j}$ and the terms $\langle\phi_i|\,\psi_j\rangle$ depend only on the difference $j-i$ of the two indices, and it also holds that

$$\langle\phi_i|\,\psi_j\rangle = \langle\psi_i|\,\Phi^{-1/2}\,|\psi_j\rangle = \langle\psi_i|\,\phi_j\rangle = \langle\psi_{i+l}|\,\phi_{j+l}\rangle. \tag{39}$$

Therefore, each term with a given k in the first sum, will be exactly cancelled by the term with $l = i+j-k$ in the second sum (recall that addition in indices is modulo N). Therefore the whole sum vanishes. We can see this by first noting that

$$\begin{aligned} \langle\phi_i|\,\psi_l\rangle\,\langle\psi_l|\,\phi_j\rangle &= \langle\phi_i|\,\psi_{i+j-k}\rangle\,\langle\psi_{i+j-k}|\,\phi_j\rangle = \\ = \langle\phi_k|\,\psi_j\rangle\,\langle\psi_i|\,\phi_k\rangle &= \langle\psi_k|\,\phi_j\rangle\,\langle\phi_i|\,\psi_k\rangle. \end{aligned} \tag{40}$$

What remains is to show that $C_{i,k} = C_{j,l}$ for $l = i+j-k$. This is the case because by assumption the cost matrix is both circulant and symmetric,

$$C_{j,l} = C_{j,i+j-k} = C_{k,i} = C_{i,k}. \tag{41}$$

■

We now proceed to investigate when the fourth Helstrom condition holds.

Theorem 2 *Consider a collection of N equiprobable symmetric states $|\psi_i\rangle$. If the cost matrix C is (1) symmetric, $C_{i,j} = C_{j,i}$, (2) circulant, $C_{i,i+k} = C_{j,j+k} = c_k$, (3) the coefficients c_k are non-positive, $c_k \leq 0 \quad \forall \quad k$ and (4) the cost matrix is negative semidefinite (its eigenvalues are all non-positive), then the SRM satisfies the inequality Helstrom condition for the minimum-cost measurement for the above cost matrix. Therefore, since the first three conditions are satisfied by theorem 1, the SRM is the minimum-cost measurement.*

Proof:
First, note that the eigenvalues of a circulant matrix are given by the discrete Fourier transform of the coefficients c_k. Thus the fourth condition of the above theorem reads

$$\bar{c}_n = \sum_{k=0}^{N-1} c_k \exp(2\pi I k n/N) \leq 0 \quad \forall \quad n. \tag{42}$$

The Helstrom inequality condition is

$$\sum_{k=0}^{N-1} \eta_j C_{j,k}\rho_k - \sum_{i,k=0}^{N-1} \eta_i \Pi_i C_{i,k}\rho_k \geq 0, \tag{43}$$

where $\eta_i = 1/N$. To prove that the operator in the LHS is positive definite, we need to prove that if we "sandwich" it with any general state $|\chi\rangle$, this always gives a positive number. We write

$$|\chi\rangle = \sum_{k=0}^{D-1} a_k\,|\gamma_k\rangle\,, \tag{44}$$

where $|\gamma_k\rangle$ is the D-dimensional orthonormal basis that we used earlier, that is, the Fourier transform of the basis $|\phi_i\rangle$ of the SRM. The Helstrom inequality condition becomes

$$\begin{aligned} &\sum_{j=0}^{N-1}\sum_{k_1,k_2=0}^{D-1} C_{i,j} a^*_{k_1} a_{k_2}\,\langle\gamma_{k_1}|\,\psi_j\rangle\,\langle\psi_j|\,\gamma_{k_2}\rangle - \\ &- \sum_{m,j}^{N-1}\sum_{k_1,k_2}^{D-1} C_{m,j} a^*_{k_1} a_{k_2}\,\langle\gamma_{k_1}|\,\phi_m\rangle\,\langle\phi_m|\,\psi_j\rangle\,\langle\psi_j|\,\gamma_{k_2}\rangle \geq 0. \end{aligned} \tag{45}$$

We use the same definitions of $\Pi_i, |\phi_i\rangle\,, |\psi_i\rangle$ as in the previous section. Moreover, note that since the cost matrix is circulant and symmetric, we have

$$c_k = C_{i,i+k} = C_{i+k,i} = C_{i,i-k} = c_{-k}. \tag{46}$$

We call the first term of eq. (45) A and the second term B. By using the definitions we obtain

$$\begin{aligned} A &= 1/N \sum_{j=0}^{N-1} \sum_{k_1,k_2=0}^{D-1} C_{i,j} a^*_{k_1} a_{k_2} \sqrt{\lambda_{k1}\lambda_{k_2}} \exp(2\pi I(k_1-k_2)j/N) \\ &= 1/N \sum_{l=0}^{N-1} \sum_{k_1,k_2=0}^{D-1} c_l a^*_{k_1} a_{k_2} \sqrt{\lambda_{k1}\lambda_{k_2}} \exp(2\pi I(k_1-k_2)(l+i)/N), \end{aligned} \tag{47}$$

where on the second line, we have used $l = j - i$ and $C_{i,i+l} = c_l$. We also obtain

$$\begin{aligned} B &= 1/N^2 \sum_{m,j=0}^{N-1} \sum_{k_1,k_2=0}^{D-1} C_{m,j} a^*_{k_1} a_{k_2} \exp(2\pi I k_1 m/N) \times \\ &\quad \times \left(\sum_{k_3=0}^{D-1} \sqrt{\lambda_{k_3}} \exp(2\pi I k_3 (j-m)/N) \right) \sqrt{\lambda_{k_2}} \exp(-2\pi I k_2 j/N) \\ &= 1/N^2 \sum_{k_1,k_2,k_3=0}^{D-1} a^*_{k_1} a_{k_2} \sqrt{\lambda_{k_2}\lambda_{k_3}} \times \\ &\quad \times \sum_{m,j=0}^{N-1} C_{m,j} \exp(2\pi I m(k_1-k_3)/N) \exp(2\pi I j(k_3-k_2)/N). \end{aligned} \tag{48}$$

Writing $C_{m,j} = c_l$, where $l = m + l$, and using the fact that $\sum_m \exp(2\pi I m(k_1 - k_2)/N) = N\delta_{k_1,k_2}$, we obtain

$$\begin{aligned} B &= 1/N^2 \sum_{k_1,k_2,k_3=0}^{D-1} a^*_{k_1} a_{k_2} \sqrt{\lambda_{k_2}\lambda_{k_3}} \times \\ &\quad \times \sum_{m,l=0}^{N-1} c_l \exp(2\pi I m(k_1-k_3)/N) \exp(2\pi I (m+l)(k_3-k_2)/N) \qquad (49) \\ &= 1/N \sum_{k_1,k_3=0}^{D-1} |a_{k_1}|^2 \sqrt{\lambda_{k_1}\lambda_{k_3}} \left[\sum_{l=0}^{N-1} c_l \exp(2\pi I l(k_3-k_1)/N) \right]. \qquad (50) \end{aligned}$$

We now take $A - B$, renaming k_3 as k_2,

$$\begin{aligned} A - B &= 1/N \sum_{k_1,k_2=0}^{D-1} \sqrt{\lambda_{k_1}\lambda_{k_2}} \left[\sum_{l=0}^{N-1} c_l \exp(2\pi I l(k_1-k_2)/N) \right] \times \\ &\quad \times \left[a^*_{k_1} a_{k_2} \exp(2\pi I i(k_1-k_2)/N) - |a_{k_1}|^2 \right]. \end{aligned} \tag{51}$$

The above expressions followed since $C_{i,j}$ is symmetric, which implies that

$$\bar{c}_n = \sum_{l=0}^{N-1} c_l \exp(2\pi I l n/N) = \bar{c}_{-n}. \tag{52}$$

The fourth condition of the theorem states that $\bar{c}_n$, the eigenvalues of the cost matrix, are always negative. Therefore Eq. (45) can further be written as (note that the remaining sums, in the following equations, take values from $k = 0$

to $k = D-1$)

$$\begin{aligned}
&\sum_{k_1,k_2} |\bar{c}_{k_1-k_2}|\sqrt{\lambda_{k_1}\lambda_{k_2}}\left(|a_{k_1}|^2 - a^*_{k_1}a_{k_2}\exp(2\pi Ii(k_1-k_2)/N)\right)\\
&= \frac{1}{2}\sum_{k_1,k_2} |\bar{c}_{k_1-k_2}|\sqrt{\lambda_{k_1}\lambda_{k_2}}\times\\
&\times\left(|a_{k_1}|^2 + |a_{k_2}|^2 - a^*_{k_1}a_{k_2}\exp(2\pi Ii(k_1-k_2)/N) - a_{k_1}a^*_{k_2}\exp(-2\pi Ii(k_1-k_2)/N)\right)\\
&= \frac{1}{2}\sum_{k_1,k_2} |\bar{c}_{k_1-k_2}|\sqrt{\lambda_{k_1}\lambda_{k_2}}\left(|a_{k_1}|^2 + |a_{k_2}|^2 - 2Re[a^*_{k_1}a_{k_2}\exp(2\pi Ii(k_1-k_2)/N)]\right)\\
&\geq \frac{1}{2}\sum_{k_1,k_2} |\bar{c}_{k_1-k_2}|\sqrt{\lambda_{k_1}\lambda_{k_2}}\left(|a_{k_1}|^2 + |a_{k_2}|^2 - 2|a_{k_1}||a_{k_2}|\right)\\
&= \frac{1}{2}\sum_{k_1,k_2} |\bar{c}_{k_1-k_2}|\sqrt{\lambda_{k_1}\lambda_{k_2}}(|a_{k_1}| - |a_{k_2}|)^2 \geq 0
\end{aligned} \tag{53}$$

which completes the proof. Note that (a) we have multiplied the expressions with N, (b) in the second line we used the general property $\sum_{k_1,k_2} L_{k_1,k_2} = 1/2\sum_{k_1,k_2}(L_{k_1,k_2} + L_{k_2,k_1})$, where L was the full expression in the sum over k_1, k_2, and (c) the inequality from the third to te forth line comes from the property $Re[z_1 z_2] \leq |z_1||z_2|$ of complex numbers.■

To illustrate what conditions on c_k's are imposed by the requirement that the eigenvalues of the cost matrix are all non-positive, we consider the case $N = 4$:

$$\begin{aligned}
\bar{c}_0 &= c_0 + c_2 + 2c_1\\
\bar{c}_1 &= c_0 - c_2\\
\bar{c}_2 &= c_0 + c_2 - 2c_1\\
\bar{c}_3 &= c_0 - c_2 = \bar{c}_1,
\end{aligned} \tag{54}$$

where we have used that $c_1 = c_3$. Given that $c_0, c_1, c_2, c_3 \leq 0$, the SRM will be the minimum-cost measurement for this cost matrix, if

$$c_2 \geq c_0 \text{ and } c_1 \geq \frac{c_0 + c_2}{2}. \tag{55}$$

C. Example: Bounding the minimum cost using SRM for coherent symmetric states

Here we will consider an example of four symmetric coherent states, given by $\{|\alpha\rangle, |i\alpha\rangle, |-\alpha\rangle, |-i\alpha\rangle\}$, for amplitude $\alpha = 2$. This symmetric set of states occurs in an implementation of quantum digital signatures [19]. The choice of protocol parameters, such as signature length, in order to guarantee sufficient security, depends on the ability of a malevolent party to forge a message. This in turn depends on the minimum cost of the best measurement a malevolent party could make on all signature copies they can obtain. In finding a bound for how well signed messages can be forged, it is crucial to bound the minimum cost for a generic cost matrix (which in general comes from experimental parameters). We will give a method for how to obtain such bounds, using, as an example, a cost matrix that was actually obtained in an experiment on quantum digital signatures [1] [19]. This cost matrix is given by

$$C = \begin{pmatrix}
9.34\times10^{-5}, & 7.81\times10^{-4}, & 1.19\times10^{-3}, & 8.70\times10^{-4}\\
9.53\times10^{-4}, & 3.25\times10^{-4}, & 9.74\times10^{-4}, & 1.36\times10^{-3}\\
1.43\times10^{-3}, & 1.40\times10^{-3}, & 6.35\times10^{-5}, & 9.61\times10^{-4}\\
8.10\times10^{-4}, & 1.62\times10^{-3}, & 9.38\times10^{-4}, & 7.07\times10^{-5}
\end{pmatrix}. \tag{56}$$

One can of course numerically compute the minimum cost using semi-definite programming. However, here we provide some analytical bounds using the properties we derived above, and the expressions for the SRM.

---

[1] The actual data that was used in that work was slightly different. The technique used to bound the forging probability was similar, but not identical, to the one presented here. We chose to use this data to better illustrate the use of the results presented in this paper.

Before attempting to bound the minimum cost, we will first compute the SRM states $|\phi_i\rangle$ for this case and the corresponding minimum-error probability. The elements of the Gram matrix are given by

$$\begin{aligned} \langle\alpha|\,\alpha\rangle = 1 \;\;,\quad & \langle\alpha|\,i\alpha\rangle = \exp(-\alpha^2(1-i)), \\ \langle\alpha|\,-\alpha\rangle = \exp(-2\alpha^2) \;\;,\quad & \langle\alpha|\,-i\alpha\rangle = \exp(-\alpha^2(1+i)). \end{aligned} \tag{57}$$

Its eigenvalues are calculated as

$$\lambda_1 = 2\exp(-\alpha^2)(\cos(\alpha^2)+\cosh(\alpha^2)) \tag{58}$$
$$\lambda_2 = 2\exp(-\alpha^2)(\sin(\alpha^2)+\sinh(\alpha^2)) \tag{59}$$
$$\lambda_3 = 2\exp(-\alpha^2)(\cosh(\alpha^2)-\cos(\alpha^2)) \tag{60}$$
$$\lambda_4 = 2\exp(-\alpha^2)(\sinh(\alpha^2)-\sin(\alpha^2)). \tag{61}$$

From this we can now write the states $|\phi\rangle$ using the Fourier orthonormal basis $|\gamma_k\rangle$,

$$|\phi_j\rangle = \frac{1}{\sqrt{N}}\sum_i \exp(2\pi I i j/N)\,|\gamma_i\rangle\,, \tag{62}$$

and the $B_{i,j}$ as

$$B_{i,j} = \frac{1}{16}|\sum_l \sqrt{\lambda_l}\exp(2\pi I(j-i)l/4)|^2. \tag{63}$$

The minimum error is then given by

$$p_{min} = 1 - 1/16|\sum_i \sqrt{\lambda_i}|^2 = 0.000168. \tag{64}$$

We now return to the minimum-cost measurement for the cost matrix in Eq. (56). In order to analytically bound the minimum cost using the methods given in the previous sections, we follow five steps.

1. We rewrite the cost matrix C as sum of a constant-row matrix C^h and the smallest possible non-negative remaining matrix C'. This is achieved by subtracting, from all elements of each row, the smallest element on that row. The cost for the constant-row matrix C^h is the smallest cost one can possibly obtain, even if one knows what state is actually sent, and is given by $\bar{C}^h \sum_i \eta_i \min_j C_{i,j}$. For our example, the smallest cost in every row is on the diagonal. Thus the cost for C^h is $\bar{C}^h = 1/4\sum_i C_{i,i} = 1.38\times10^{-4}$. We obtain the matrix

$$C' = \begin{pmatrix} 0, & 6.88\times10^{-4}, & 1.10\times10^{-3}, & 7.77\times10^{-4} \\ 6.28\times10^{-4}, & 0, & 6.49\times10^{-4}, & 1.04\times10^{-3} \\ 1.37\times10^{-3}, & 1.34\times10^{-3}, & 0, & 8.98\times10^{-4} \\ 7.39\times10^{-4}, & 1.55\times10^{-3}, & 8.68\times10^{-4}, & 0 \end{pmatrix}. \tag{65}$$

2. We further subtract the greatest fully constant matrix with $C^c_{i,j} = M$ for all i,j, so that the remaining cost matrix is strictly non-positive, i.e. $C'_{i,j} = M + C''_{i,j}$. This means subtracting, from all elements $C'_{i,j}$, the greatest element in that matrix. For our example, the greatest element is $1.55\times10^{-3} = M$, and this leads to (note the minus sign outside the matrix)

$$C'' = -\begin{pmatrix} 1.55\times10^{-3}, & 0.86\times10^{-3}, & 0.45\times10^{-3}, & 0.77\times10^{-3} \\ 0.92\times10^{-3}, & 1.55\times10^{-3}, & 0.90\times10^{-3}, & 0.51\times10^{-3} \\ 0.18\times10^{-3}, & 0.21\times10^{-3}, & 1.55\times10^{-3}, & 0.65\times10^{-3} \\ 0.81\times10^{-3}, & 0, & 0.68\times10^{-3}, & 1.55\times10^{-3} \end{pmatrix}. \tag{66}$$

   The overall cost so far is $\bar{C}(\Pi) = \bar{C}^h + M + \bar{C}''(\Pi)$, where the cost of C'' is a function of the measurement made, and takes a negative value, since all the elements of the matrix are negative.

3. The cost of any cost matrix which is smaller, element by element, than C'', bounds the overall cost from below. To find the tightest bound, we look for such a matrix with the largest possible elements, which also satisfies the conditions of theorem 2, so that the minimum cost is given by the SRM. For our example, the largest cost matrix which is smaller than C'' and is circulant, symmetric and has negative eigenvalues, is given

by $C^l = \{c_0 = -1.55 \times 10^{-3}, c_1 = -0.92 \times 10^{-3}, c_2 = -0.51 \times 10^{-3}\}$. Note that the condition for negative eigenvalues is satisfied, $c_2 \geq c_0$ and $c_1 \geq \frac{c_0+c_2}{2}$. It follows that the SRM gives the minimum cost for C^l, and this cost is $\bar{C}^l_{min} = -1.54989 \times 10^{-3}$. This gives a lower bound for the minimum cost of C,

$$\bar{C}_{min} \geq \bar{C}^h + M + \bar{C}^l_{min} = 1.38 \times 10^{-4} + 1.1 \times 10^{-7}. \tag{67}$$

4. Similarly, to find an upper bound, we seek a cost matrix which is larger than C'', element by element, which is the smallest possible matrix which also satisfies the conditions of theorem 2. This matrix is given by $C^u = \{c_0 = -1.55 \times 10^{-3}, c_1 = -0.21 \times 10^{-3}, c_2 = 0\}$. We can also confirm that its eigenvalues are negative, since the conditions for this are satisfied. Therefore the SRM is the minimum-cost measurement for C^u, with the cost $\bar{C}^u_{min} = -1.54978 \times 10^{-3}$. This leads to an upper bound for the minimum cost of C as

$$\bar{C}_{min} \leq \bar{C}^h + M + \bar{C}^u_{min} = 1.38 \times 10^{-4} + 2.2 \times 10^{-7}. \tag{68}$$

We therefore obtain the bounds

$$1.38 \times 10^{-4} + 2.2 \times 10^{-7} \geq \bar{C}_{min} \geq 1.38 \times 10^{-4} + 1.1 \times 10^{-7}. \tag{69}$$

We see that these bounds are relatively tight. The minimum cost is of the order of 10^{-4}, while the accuracy that the minimum cost is bounded by is of order 10^{-7}. Another point to mention is that in the case the cost matrix after subtracting the constant-row C^h is circulant, then it is likely that the two bounds coincide. In other words, in that case we obtain the exact minimum cost. A final point to stress here is that both the upper and lower bounds are important for different type of circumstances. If, for example, the minimum cost corresponds to the probability that some malevolent party correctly guesses the state, thereby undermining the security of some cryptographic protocol, then we are interested in the worst-case scenario, which is that he makes the best possible guess. We then use the lower bound of the minimum cost in order to make sure that our protocol is secure. If, on the other hand, some honest party is required to make the guess, then the worst case scenario corresponds to the upper bound for the minimum cost.

V. MINIMUM-ERROR MEASUREMENT AND PROBABILITIES FOR MIXED STATES OF SYMMETRIC PURE STATES

In the previous section we have seen that the minimum-cost measurement for a wide class of cost matrices for symmetric pure states is the SRM. More specifically, using the results of section II, we see that if we can make a cost matrix circulant, with non-positive entries and negative semidefinite, by adding (subtracting) constant-row matrices, then the minimum-cost measurement is the SRM. Moreover, the cost can be easily analytically computed using the expressions for the SRM in terms of the eigenvalues of the Gram matrix of the symmetric states.

Here we will use the above result, and the equivalence between minimum-cost measurements for pure states and minimum-error measurements for mixed states, which we discussed in section III, to obtain the minimum-error probability for a class of mixed states which are mixtures of pure symmetric states. We will similarly provide bounds on the minimum-error probability for a larger class of mixed states.

The first observation is that for any collection of mixed states of the form $\bar{\rho}_i = \sum_j a_{i,j} |\psi_j\rangle \langle\psi_j|$, where $|\psi_j\rangle$ are symmetric states, we can rephrase any constraints (for a given measurement to be optimal) on the cost matrix with elements $C_{i,j}$ in terms of conditions on the $a_{i,j}$. In particular, assuming for simplicity that the prior probabilities η_i of the different mixed states $\bar{\rho}_i$ are all equal to $1/N$, we obtain

$$a_{i,j} = 1 - C_{j,i}. \tag{70}$$

Requiring that the cost matrix C is symmetric and circulant implies that the matrix with elements $a_{i,j}$ should also be symmetric and circulant, while requiring that the cost matrix C is negative semidefinite, implies the requirement that $a_{i,j}$ define a positive semidefinite matrix. The results in the previous section imply that if the states $\bar{\rho}_i$ are such that the $a_{i,j}$ define a circulant, symmetric and positive definite matrix, then the SRM is the minimum-error measurement for the mixed states $\bar{\rho}_i$'s.

An interesting thing to point out is that mixed states generated by a circulant, symmetric matrix $a_{i,j}$, from pure symmetric states, are also symmetric states, induced by the same symmetry unitary. We can see that, since

$$U\bar{\rho}_i U^\dagger = \sum_j a_{i,j} U^\dagger |\psi_j\rangle \langle\psi_j| U^\dagger = \sum_j a_{i,j} |\psi_{j+1}\rangle \langle\psi_{j+1}| \tag{71}$$

$$= \sum_j a_{i+1,j+1} |\psi_{j+1}\rangle \langle\psi_{j+1}| = \sum_j a_{i+1,j} |\psi_j\rangle \langle\psi_j| = \bar{\rho}_{i+1}. \tag{72}$$

We have therefore shown that the SRM is the minimum-error measurement, even for mixed symmetric states defined as above, provided the eigenvalues of $a_{i,j}$ are non-negative. This is in agreement with the result of ref. [8].

An other interesting consequence concerns the case where the mixed states are arbitrary mixtures of symmetric states. In other words, when the matrix defined by $a_{i,j}$ is more general. As we have outlined in the example in the previous section, we are able to provide upper and lower bounds for the minimum error of those mixed states (given by the minimum cost for the corresponding pure states), using the explicit and easy form of the SRM for symmetric pure states. In particular, if those bounds are accurate, compared to other significant parameters that may interest us, then we can use the bounds provided by the SRM to estimate the minimum-error probability for the mixed states.

Finally, one should note that if the analytical form of the minimum-cost measurement for some class of cost matrices is known (as in our examples the SRM), then one can obtain bounds for the minimum error for a related class of mixed states using the methods we described.

VI. MINIMUM COST FOR SEQUENCES OF STATES

In this section we will consider tensor products of states. In particular, we will focus on a special case, which is important for quantum cryptography. The Hilbert space is a tensor product of identical Hilbert spaces $\mathcal{H}_{tot} = \otimes_{i=1}^{L} \mathcal{H}_i$. We refer to the whole state as global, and the individual states as local. The set of possible states that we are going to consider consists of all (tensor product) combinations of the N different local states, for the L different subsystems that make the global state.

Such states occur frequently in quantum information science. The local states comprise an alphabet of possible quantum "letter" states, whereas the total tensor product state form a quantum "message". Such states occur in, for example, QKD, where the total system Alice sends to Bob is a sequence of L local states. In BB84, the local states belong to two mutually unbiased bases. Appropriately ordered, the states form a set of symmetric states. Analogous situations occur in quantum digital signatures, universal blind quantum computing, and other protocols. Considering the entire global system, as opposed to individual components, which was the topic of previous sections, leads to collective (or coherent) measurement strategies which can be uses to gain information about the system.

To each individual local system one can assign a local minimum-cost problem, which is the situation we discussed previously. From the collection of local problems, one can derive a global minimum-cost problem, where the global cost is some function of local costs. A typical example of this is the scenario in which a party wishes to identify the message sent, in a way which minimizes the number of local states for which a misidentification occurred. In this paper we will consider the more general case of global cost matrices where the cost for each global state is some (general) function of the sum of the (local) costs of the subsystems. We further assume that the local cost matrices are all identical for the different subsystems. This type of systems and cost matrices are widely used.

The question of whether the optimal measurement is a tensor product of local measurements, in scenarios where the possible states are tensor product states, was crucial in the development of QKD. The optimal measurement for obtaining the parity of a bit string, in the context of QKD, was examined by Fuchs and Graaf in [25] and by Bennett, Mor and Smolin in [26]. It turns out that whether or not a sequence of local measurements is optimal depends on the global cost matrix, that is, on the specific global cost function. In particular, it was shown that the parity of a string of bits, encoded in qubits as in the BB84 protocol, can be best guessed by measuring in an entangled basis. The parity of a string is equal to addition modulo 2 of the bits, and the global cost becomes a function of the local costs.

It may seem counter-intuitive that entangled measurements outperform local ones, since the possible states are all tensor products, and there are no correlations between individual bits or qubits in the example with the parity. However, for correctly determining the parity of the string of bits in this example, there is no optimum "local" measurement strategy. If we obtain the correct bit value after measuring the first qubit, then the best strategy is to guess the second bit correctly. But if we have guessed the first bit wrong, it is beneficial to make another mistake for the second one so that the parity is guessed correctly. The overall cost is a periodic function of the sum of the local costs. What is more surprising, however, is that even if the global cost is a monotone function of the local costs, then it is still not guaranteed that the global optimal measurement is non-entangled.

In this section we will first prove that for a total cost matrix which is a linear function of the sum of the local costs, the minimum-cost measurement is a tensor product of local measurements. We will then provide bounds for total costs which are convex and concave functions of the sum of local costs. Finally we will give an example of a monotone function, a step function, for which the minimum-cost measurement is a measurement in an entangled basis. This example is interesting for various reasons. First, this type of cost matrix appears in protocols for QDS. Second, it is closely related to conclusive state elimination [21, 22]. Third, this type of measurement is the one used to argue that an epistemic view of the wavefunction is impossible [20].

We should introduce some notation here. The total number of local subsystems is L, and we call the global space of

all subsystems Ω. We label the global possible states as $\rho_k^{tot} = \otimes_i \rho_{k(i)}$. We will use the index k for the global space, that is, it takes N^L different values. To refer to different such global states, we will use subscripts (e.g. $k_1, k_2, \cdots$). When we want to refer to the state of a particular subsystem, e.g. the i'th, we will write $k(i)$. We assume that each subsystem is identical, and has N different possible states. The states of the subsystems are independent of each other, so that the prior probabilities for the global states can be written as products $\eta_k^{tot} = \prod_i \eta_{k(i)}$. Note that $\sum_{k(i)} \eta_{k(i)} = 1$ for all i, since the probabilities of each subsystem sum to one.

The cost matrices we are considering have entries of the form $C_{k_1,k_2} = f(\sum_i C^i_{k_1(i),k_2(i)})$. C_{k_1,k_2} is the cost of choosing outcome k_2 if the global state was ρ_{k_1}. $C^i_{k_1(i),k_2(i)}$ are the entries of the local cost matrices. The cost of a global measurement corresponding to a POVM Π with elements $\{\Pi_k\}$ is given by

$$\bar{C}(\Pi) = \sum_{k_1,k_2} \eta_{k_1} C_{k_1,k_2} Tr(\Pi_{k_2} \rho_{k_1}). \tag{73}$$

Indices in the above take values from one to N^L, as they will always do, unless the particular element is specified. For example, $k_1(i)$ is the index for the i'th subsystem, in the sequence k_1. The task here is to find under what conditions on C_{k_1,k_2} (which is in our case is a function of the sum of the local costs) the minimum-cost measurement is to make optimal local minimum-cost measurements. For those cases, the value of the minimum cost can also be computed.

A. Cost matrix in the form of a linear function of the sum of local costs

Theorem 3 *Assume a set of product states with independent prior probabilities for the subsystems. Assume that the global cost matrix C_{k_1,k_2}, is a linear function of the sum of some local cost matrices entries $C^i_{k_1(i),k_2(i)}$. In other words,*

$$C_{k_1,k_2} = f\left(\sum_i C^i_{k_1(i),k_2(i)}\right) = a \sum_i C^i_{k_1(i),k_2(i)} + b \tag{74}$$

with $f(x) = ax + b$. Then (i) the minimum-cost measurement is the tensor product of the local minimum-cost measurements for the local costs C^i and (ii) the minimum cost is given as $\bar{C}_{min} = a \sum_i \bar{C}^i_{min} + b$.

In order to prove the above theorem, we first need few lemmas.

Lemma 4 *Consider a subset A of Ω that consists of a collection of local subspaces $i \in A$ and call $\bar{A} = \Omega \setminus A$. The Hilbert space associated with A is $\mathcal{H}_A = \otimes_{i\in A}\mathcal{H}_i$. Assume that the global cost matrix depends only on $i \in A$, i.e. $C_{k_1,k_2} = f(i \in A)$. Then for any global measurement $\Pi \in \mathcal{H}_{tot}$, there exists another measurement of the form $\bar{\Pi}_A \otimes \mathbb{I}_{\bar{A}}$, with $\bar{\Pi} \in \mathcal{H}_A$, that gives the same cost $\bar{C}(\Pi_\Omega) = \bar{C}(\bar{\Pi}_A \otimes \mathbb{I}_{\bar{A}})$.*

Proof:
First we should note that the prior probabilities are of the form $\eta_k = \eta_{k(A)}\eta_{k(\bar{A}')}$, i.e. independent for $\mathcal{H}_A$ and $\mathcal{H}_{\bar{A}}$. We will prove the lemma by explicit construction. From eq. (73) we obtain the following expression for the cost, where the subscripts for the POVMs indicate on which subsystems they act,

$$\begin{aligned}\bar{C}(\Pi_\Omega) \;=\; & \sum_{k_1(A),k_1(\bar{A})} \sum_{k_2(A),k_2(\bar{A})} C_{k_1(A),k_2(A)} \eta_{k_1(A)} \eta_{k_1(\bar{A})} \times \\ & \times Tr\left(\Pi_{k_2(A),k_2(\bar{A})} \rho_{k_1(A)} \otimes \rho_{k_1(\bar{A})}\right).\end{aligned} \tag{75}$$

An important thing to note is that the sums in Eq. (73) run over all k_1, k_2, where we have decomposed these sums to summing over the different possibilities for the subsystems (summing over $k_1(A), k_1(\bar{A}), k_2(A), k_2(\bar{A})$). The operator Π_{k_2} has also been expressed as function of $k_2(A)$ and $k_2(\bar{A})$, without implying that it has product structure. Finally, note that the cost matrix, by the assumptions in the lemma, depends only on the indices belonging to A.

By defining a POVM which acts on $\mathcal{H}_A$ (note the partial trace) as

$$\bar{\Pi}_{k_2(A)} = Tr_{\bar{A}}\left(\Pi_{k_2} \cdot \mathbb{I}_A \otimes \left(\sum_{k_1(\bar{A})} \eta_{k_1(\bar{A})} \rho_{k_1(\bar{A})}\right)\right), \tag{76}$$

it follows that the lemma holds since one can easily check that

$$\bar{C}(\Pi_\Omega) = \bar{C}(\bar{\Pi}_A \otimes \mathbb{I}_{\bar{A}}). \tag{77}$$

Therefore, for all possible costs, one can find a measurement acting non-trivially only on $\mathcal{H}_A$, achieving that cost. In the cases described by this lemma, with no loss of generality, for any optimization we can restrict out attention to measurements acting on $\mathcal{H}_A$.■

Lemma 5 *If the cost matrix depends only on a subsystem A, i.e. $C_{k_1,k_2} = f(i \in A)$, and we have any measurement with a POVM of the form $\Pi_A \otimes \Pi_{\bar{A}}$, then the cost of the measurement is independent of the measurement on subsystem $\bar{A}$, that is,*

$$\bar{C}(\Pi_A \otimes \Pi_{\bar{A}}) = \bar{C}(\Pi_A \otimes \Pi'_{\bar{A}}) = \bar{C}(\Pi_A \otimes \mathbb{I}_{\bar{A}}). \tag{78}$$

Proof:
Since both the state and the elements of the POVM, are factorizable, the trace is simply the product of the trace of the subsystems $A, \bar{A}$, and Eq. (73) becomes

$$\begin{aligned}\bar{C}(\Pi_A \otimes \Pi_{\bar{A}}) &= \sum_{k_1(A),k_2(A)} \eta_{k_1(A)} C_{k_1(A),k_2(A)} Tr\left(\Pi_{k_2(A)} \rho_{k_1(A)}\right) \times \\ &\quad \times \left(Tr\left(\sum_{k_1(\bar{A}),k_2(\bar{A})} \Pi_{k_2(\bar{A})} \rho_{k_1(\bar{A})} \right) \right) = \\ &= \sum_{k_1(A),k_2(A)} \eta_{k_1(A)} C_{k_1(A),k_2(A)} Tr\left(\Pi_{k_2(A)} \rho_{k_1(A)}\right), \end{aligned} \tag{79}$$

where we have used the fact that C_{k_1,k_2} is independent of $k_1(\bar{A})$ and $k_2(\bar{A})$ to move the second sum in (75) inside the trace, and also that $\sum_{k_2(\bar{A})} \Pi_{k_2(\bar{A})} = \mathbb{I}_{\bar{A}}$, the trace of the density matrix is one and $\sum_{k_1(\bar{A})} \eta_{k_1(\bar{A})} = 1$.■

Lemma 6 *If the global cost is constant function ($f(x) = C$) and therefore $C_{k_1,k_2} = C$, then all measurements give same cost equal to that constant C.*

This follows from the definition of cost.

Lemma 7 *Consider a global cost matrix that is equal to the sum of the local cost matrices $C_{k_1,k_2} = \sum_i C^i_{k_1(i),k_2(i)}$ (corresponds to the case of a function $f(x) = x$ of the sum of the individual cost matrices). Then, the minimum-cost measurement is given by tensor product of local minimum-cost measurements. Moreover the minimum cost is given by $\bar{C}_{min} = \sum_i \bar{C}^i_{min}$.*

Proof:
Eq. (73) can be rewritten as

$$C(\Pi) = \sum_{k_1,k_2} \eta_{k_1} (\sum_i C^i_{k_1(i),k_2(i)}) Tr(\Pi_{k_2} \rho_{k_1}) = \sum_i C^i(\Pi), \tag{80}$$

where we defined

$$C^i(\Pi) = \sum_{k_1,k_2} (\eta_{k_1}) C^i_{k_1(i),k_2(i)} Tr(\Pi_{k_2} \rho_{k_1}). \tag{81}$$

Intuitively, each C^i corresponds to a cost matrix that has no cost for any declaration for any subsystems except for subsystem i. The minimum cost of C^i is denoted by $\bar{C}^i_{min}$. By noting that each C^i depends only on the i'th element and using lemma 4, we have

$$\bar{C}^i_{min} = \bar{C}^i(\Pi^{min}_i \otimes \mathbb{I}_{\Omega\setminus\{i\}}) = \bar{C}^i(\Pi^{min}_i \otimes \Pi_{\Omega\setminus\{i\}}), \tag{82}$$

where $\Pi_{\Omega\setminus\{i\}}$ is any element of a POVM acting on that space, and the second equality follows from Lemma 5. Moreover, from Lemma 2, it follows that the minimum total cost cannot be less than the sum of the minimum costs of each term in the sum. However, since for each term of the sum we have a measurement that has relevant support only on one subspace (the measurement on the remaining subsystems can be arbitrary), it is possible to have a measurement that achieves the minimum cost for all terms simultaneously, and thus the lower bound of lemma 2 can actually be achieved. The measurement is given by the operators $\otimes_i \Pi^{min}_i$, and gives the cost $\bar{C}_{min} = \sum \bar{C}^i_{min}$.■
Note that we have shown that there exists a minimum cost measurement that is local. Since the optimal measurement is not unique, there may also be non-local measurement that achieves the same minimum cost.

Finally, it follows that Theorem 3 holds from the last two lemmas and the definition of the cost matrix.

B. Convex, concave, monotonic and general functions

Here we will consider bounds and statements which apply when the global cost matrix is a general function of the sum of some local costs.

Lemma 8 *Assume that we have a global cost matrix that is a convex function of the sum of some local costs* $C_{k_1,k_2} = f(\sum_i C^i_{k_1(i),k_2(i)})$. *Then the global minimum cost is upper bounded by the sum of local minimum costs,*

$$C_{min} \leq \sum_i f(C^i_{min}). \tag{83}$$

Proof:
This follows by noting that $f((1/N)\sum_i C^i_{k_1(i),k_2(i)}) \leq (1/N)\sum_i f(C^i_{k_1(i),k_2(i)})$, and by Lemma 7, which says that the minimum cost, for a global cost function which is a sum of local costs, is given by the sum of the local minimum costs for local cost functions $(1/N)f(C^i_{k_1(i),k_2(i)})$. The minimum cost obtained by making the local optimal measurements is therefore greater than or equal to the minimum possible cost for the cost function $C_{k_1,k_2} = f(\sum_i C^i_{k_1(i),k_2(i)})$, and thus provides an upper bound for the cost we are interested in. ■

Lemma 9 *Assume that we have a global cost matrix which is a concave function of the sum of some local costs,* $C_{k_1,k_2} = f(\sum_i C^i_{k_1(i),k_2(i)})$. *Then the global minimum cost is lower bounded by the sum of local minimum costs,*

$$C_{min} \geq \sum_i f(C^i_{min}). \tag{84}$$

Proof:
This again follows by noting that $f((1/N)\sum_i C^i_{k_1(i),k_2(i)}) \geq (1/N)\sum_i f(C^i_{k_1(i,k_2(i))})$, and by Lemma 7. The minimum cost obtained by optimal local measurements for the local costs $(1/N)f(C^i_{k_1(i),k_2(i)})$ is less or equal to the minimum cost in question, and thus provide a lower bound for this minimum cost. ■

C. Functions for which local measurements are sub-optimal, state elimination, and the PBR argument

In this section, we will give an example, which proves that even if the function of the local costs is monotonically increasing, the minimum cost measurement is not necessarily given by local minimum-cost measurements. We will consider a cost matrix which is a step function of the sum of the local costs. A step function is an important example, since in cryptographic protocols such as QDS [16–19], a party will accept a signed message as genuine if it contains fewer mismatches than a particular threshold. This means that achieving fewer mismatches than this threshold carries no cost, since the signed message is accepted as genuine, while exceeding the threshold has cost equal to one, since the message is rejected.

Consider a sequence of two qubits, each of them is either in the state $|0\rangle$ or in the state $|+\rangle = 1/\sqrt{2}(|0\rangle + |1\rangle)$. The global cost is given by a step function of the sum of the local costs, where the local cost matrices are the error probability $C_{i,j} = 1 - \delta_{i,j}$. In particular, we will consider the case where if both bits are wrong then the cost is one, while if only one or none of the bits are wrong, then there is no cost at all. In other words, we want to be sure that we do not make mistake for both elements, but either zero or one error is fine.

The best local measurement is clearly to perform a minimum-error measurement for each qubit. The cost for this measurement is given by

$$\bar{C}(local) = p^2_{min} = (1 - 1/2(\sqrt{1 - |\langle 0|+\rangle|^2} + 1))^2 = 0.021 \tag{85}$$

which is the minimum probability of error for both (independent) elements. However, there exists a measurement in an entangled basis (we will call this the *PBR basis*), that gives a smaller cost. If we measure in the following basis,

$$|\phi_{++}\rangle = 1/\sqrt{2}(|01\rangle + |10\rangle) \tag{86}$$
$$|\phi_{+0}\rangle = 1/\sqrt{2}(|0-\rangle + |1+\rangle) \tag{87}$$
$$|\phi_{0+}\rangle = 1/\sqrt{2}(|+1\rangle + |-0\rangle) \tag{88}$$
$$|\phi_{00}\rangle = 1/\sqrt{2}(|+-\rangle + |-+\rangle), \tag{89}$$

then we will *never* make two mistakes. The cost for this measurement, $\bar{C}(PRB)$, is therefore exactly zero.

We should make two comments here. First, this measurement basis was given by Pusey, Barrett and Rudolph (PBR) [20] in an argument for proving that the nature of the wavefunction in quantum mechanics is not epistemic. Here we give a simplified version of this argument. The PBR argument started with the assumption that the wavefunction represents an epistemic distribution over some underlying different ontic states. Since the local states are non-orthogonal, they concluded that some ontic states are compatible with both $|0\rangle$ and $|+\rangle$ with some non-zero probability that is directly related to p_{min}. Having a pair of uncorrelated, non-interacting local states, would imply that there are some global ontic states, with probability p_{min}^2, that are compatible with all four possible wavefunctions $\{|00\rangle, |0+\rangle, |+0\rangle, |++\rangle\}$. However, if one measures in the PBR basis, any outcome that is obtained is incompatible with (rules out) one of the four possible initial states. This manifest itself by the fact that the $\bar{C}(PBR)$ is zero. Therefore, the assumption that the wavefunction has purely epistemic character has to be rejected. It is very interesting that this deep philosophical insight is immediately connected to the security of cryptographic protocols.

The second comment is that this exact type of measurement can be understood as quantum state elimination or quantum state exclusion [19, 21, 22]. Depending on which of the four possible outcomes is obtained, we can, with 100% probability, rule out one of the possible states. In particular, we can rule out the state for which both qubits are different compared with our result. This again is slightly counter-intuitive, since we started with four possible linearly independent non-orthogonal states. While it is well known that we cannot determine the state with certainty, we can rule out (eliminate) a state with certainty.

Finally, an interesting observation is that it is the inequality Helstrom condition that is expected to fail for the local measurements. In a sense, the local minimum-cost measurements corresonds to a "local minimum", in the sense that it is optimal compared to other slight perturbations. However, there is an entangled basis which is globally optimal. In the appendix A we see that for sequences of symmetric states with a global cost matrix which is any function of the sum of the local costs, the three first conditions of Helstrom hold for local SRMs. It is the failure of inequality condition, however, that leads to an optimal measurement in an entangled basis for certain global cost functions[2].

VII. SUMMARY AND CONCLUSIONS

In this paper we examined minimum-cost measurements in order to obtain useful tools for quantum information and quantum communications. Knowledge of optimal measurements is important for example for bounding the ability of adversaries in cryptographic protocols to forge messages or learn about a secret key. We obtained a series of results concerning minimum-cost measurements. In particular, we showed (1) that the minimum-cost measurement remains the same if we add a constant-row cost matrix to the cost matrix, (2) one can bound the minimum cost from above (below) with an element-by-element greater (smaller) cost matrix, (3) one can bound the cost for a sum of cost matrices by the sum of the minimum costs for the individual cost matrices in the sum. We also (4) derived a formal mathematical equivalence between minimum-cost measurements for pure states and minimum-error measurements for mixtures of those pure states. Then we focused on the case of symmetric states, where we (5) derived an expression for the square-root measurement (SRM) and the minimum error for pure states in terms of the eigenvalues of the Gram matrix for the states which takes a surprisingly simple form (Eq. (36)), and (6) showed that when the cost matrix is circulant, symmetric, has negative elements and is negative semidefinite, then the SRM is the minimum-cost measurement. We (7) gave a particular example, where we obtained lower and upper bounds for the minimum cost of an arbitrary cost matrix. These results lead us to (8) obtain the minimum-error probability for mixed states which are a particular kind of mixtures of pure symmetric states, and a method to bound the minimum-error probability for a larger class of mixed states.

Finally we (9) considered sequences of (that is, tensor products of) individual systems, where the global cost is a function of the local costs. We (i) showed that if this function is linear, then a combination of local minimum-cost measurements is the global minimum-cost measurement, (ii) if the function is convex or concave we obtain bounds (upper/lower) from the local minimum cost measurements. We moreover (iii) showed that this is not the case for general functions of the local costs, even if the function is monotonic, and pointed out the connection between this, quantum state elimination measurements and the PBR argument regarding the nature of the wave function.

Acknowledgments. Support by EPSRC grants EP/G009821/1, EP/K022717/1 and an EPSRC Doctoral Fellowship is gratefully acknowledged. PW is also partially supported by COST Action MP1006.

[2] Note that even in the example with a step function, it is not always the case that global measurements outperform local ones. This depends on the particular value at which the step occurs. In the example we presented, if the step function was such that we accept only if both states are correct, then the optimum measurement would be a combination of local measurements.

Appendix A: Minimum-cost measurements on tensor products of symmetric states

Consider a minimum-cost measurement on a sequence of individual symmetric states. We will here show that the first three Helstrom conditions are satisfied by the local SRMs, if the local (individual) states are symmetric, for any global cost matrix that is a function of the sum of the local costs.

We consider tensor product states of symmetric local states, where the local costs are circulant and symmetric, and the global cost is some function of the sum of the local costs. We will prove that the tensor product of local SRMs satisfies the first three Helstrom conditions. However, as expected, the inequality conditions are not in general satisfied. Here we will use the same notation and terminology as in section VI.

Theorem 4 *Assume a global tensor product state of local pure symmetric states, and a global cost matrix that is (any) function of the sum of some local cost matrices. If the local cost matrices are circulant and symmetric, then the first three Helstrom conditions hold for the measurement with measurement which is a combination of local SRMs.*

Proof:
We rewrite the minimum-cost measurement for the global system as a minimum-error measurement for newly defined states $\bar{\rho}_{k_i} = \sum_{k_j} C_{k_i,k_j}\rho_{k_j}$, with the same convention for indices as in section VI. The Helstrom condition for the minimum-error measurement is then

$$\Pi_{k_1}\left(\sum_{k_1,k_2} C_{k_1,k_3}\rho_{k_3} - \sum_{k_4} C_{k_2,k_4}\rho_{k_4}\right)\Pi_{k_2} = 0 \tag{A1}$$

for all global states labelled by k_1, k_2. By assumption, the cost matrix is of the form

$$C_{k_1,k_2} = f\left(\sum_i C_{k_1(i),k_2(i)}\right). \tag{A2}$$

We can view the sum of the local cost matrices as a distance of the string k_1 from the string k_2, and therefore the cost matrix is some function of the distance between the two states. The claim is that the tensor product of local SRMs satisfies Eq. (A1). The global states corresponding to the SRM are of the form $|\phi_k\rangle = \otimes_i \left|\phi_{k(i)}\right\rangle$ and eq. (A1) becomes

$$\sum_{k_3,k_4}\left(C_{k_1,k_3}\left\langle\phi_{k_1}\right|\left.\psi_{k_3}\right\rangle\left\langle\psi_{k_3}\right|\left.\phi_{k_2}\right\rangle - C_{k_4,k_2}\left\langle\phi_{k_1}\right|\left.\psi_{k_4}\right\rangle\left\langle\psi_{k_4}\right|\left.\phi_{k_2}\right\rangle\right) = 0. \tag{A3}$$

To prove that this holds, it is sufficient to show that each term in the first sum cancels a term in the second sum, in a way so that the whole sum vanishes. We can explicitly show that this is the case. For any given k_1, k_2, k_3, choose k_4 so that for each element $k_4(i) = k_1(i) + k_2(i) - k_3(i)$, where the addition and subtraction is done for the labels of the local symmetric states, and is done modulo N. This gives a bijective map between terms in the two sums. Since the cost matrix is a function of the sum of the local cost matrices, and the local cost matrices are circulant, the total cost matrix is also circulant and therefore

$$C_{k_4,k_2} = C_{k_1+k_2-k_3,k_2} = C_{k_1,k_3}, \tag{A4}$$

where the addition of global indices is understood as element by element addition modulo N. What remains for the proof is to show that

$$\left\langle\phi_{k_1}\right|\left.\psi_{k_3}\right\rangle\left\langle\psi_{k_3}\right|\left.\phi_{k_2}\right\rangle = \left\langle\phi_{k_1}\right|\left.\psi_{k_4}\right\rangle\left\langle\psi_{k_4}\right|\left.\phi_{k_2}\right\rangle \tag{A5}$$

for the choice of k_4 we made above. Note that

$$\begin{aligned}\left\langle\phi_{k_1(i)}\right|\left.\psi_{k_2(i)}\right\rangle &= \left\langle\psi_{k_1(i)}\right|\Phi^{-1/2}\left|\psi_{k_2(i)}\right\rangle = \\ = \left\langle\psi_{k_1(i)}\right|\left.\phi_{k_2(i)}\right\rangle &= \left\langle\psi_{k_1(i)+l}\right|\left.\phi_{k_2(i)+l}\right\rangle,\end{aligned} \tag{A6}$$

i.e. these terms are circulant. The r.h.s. of Eq. (A5) becomes

$$\begin{aligned}\prod_i \langle \phi_{k_1(i)} | \psi_{k_4(i)} \rangle \prod_{i'} \langle \psi_{k_4(i)} | \phi_{k_2(i)} \rangle &= \prod_i \langle \phi_{k_1(i)} | \psi_{k_1(i)+k_2(i)-k_3(i)} \rangle \times \\ &\quad \times \prod_{i'} \langle \psi_{k_1(i)+k_2(i)-k_3(i)} | \phi_{k_2(i)} \rangle \\ &= \prod_i \langle \phi_{k_3(i)} | \psi_{k_2(i)} \rangle \prod_{i'} \langle \psi_{k_1(i)} | \phi_{k_3(i)} \rangle \\ &= \prod_i \langle \psi_{k_3(i)} | \phi_{k_2(i)} \rangle \prod_{i'} \langle \phi_{k_1(i)} | \psi_{k_3(i)} \rangle,\end{aligned} \tag{A7}$$

using the fact that the local cost matrices are circulant. The last line is equal to the l.h.s. of Eq. (A5) which then shows that eq. (A1) holds and completes the proof.■

The important thing to note is that we did not need to make any assumptions on the exact form of the global cost function. One can explicitly check that the inequality condition also holds for linear global cost functions, which is expected due to the results of section VI. As we show, it turns out that this condition is often not satisfied, even for certain monotonic functions.

[1] Helstrom C W 1976 *Quantum detection and estimation theory*, Academic Press, New York.
[2] Clarke R B M, Kendon V M, Chefles A, Barnett S M, Riis E, and Sasaki M 2001 *Phys. Rev. A* **64** 012303
[3] Waldherr G, Dada A C, Neumann P, Jelezko F, Andersson E and Wrachtrup J 2012 *Phys. Rev. Lett.* **109** 180501
[4] Franke-Arnold S, Andersson E, Barnett S M, and Stenholm S 2001 *Phys. Rev. A* **63** 052301
[5] Andersson E, Barnett S M, Gilson C R and Hunter K 2002 *Phys. Rev. A* **65** 052308
[6] Barnett S 2001 *Phys. Rev. A* **64** 030303
[7] K. Nakahira 2012 *IEEE Transactions on Information Theory* **58** 1215
[8] Chou C-L and Hsu L-Y 2003 *Phys. Rev. A* **68** 042305
[9] Hunter K 2004 *AIP Conf. Proc.* **734** 83; Hunter K 2004 *Optimal Generalised Measurement Strategies* PhD thesis, University of Strathclyde
[10] Bae J 2013 *New J. Phys.* **15** 073037
[11] Andersson E 2012 *Phys. Rev. A* **86** 012120
[12] Bennett C and Brassard G 1984 *Proceedings of IEEE International Conference on Computers Systems and Signal Processing* pp. 175–179
[13] Barbosa G A, Corndorf E, Kumar P and Yuen H P 2003 *Phys. Rev. Lett* **90** 227901
[14] Sych D and Leuchs G 2010 *New J. Phys.* **12** 053019
[15] Broadbent A, Fitzsimons J, and Kashefi E 2009 *Proceedings of the 50th Annual IEEE Symposium on Foundations of Computer Science* (IEEE Computer Society, Los Alamitos, USA, 2009) pp. 517–526
[16] Gottesman D, and Chuang I 2001 preprint *arXiv:quant-ph*/0105032v2
[17] Clarke P J, Collins R J, Dunjko V, Andersson E, Jeffers J and Buller G S 2012 *Nat. Commun.* **3** 1174
[18] Dunjko V, Wallden P and Andersson E 2013 preprint [arXiv:1309.1375]
[19] Collins R J, Donaldson R J, Dunjko V, Wallden P, Clarke P J, Andersson E, Jeffers J and Buller G S 2013 preprint [arXiv:1311.5760]
[20] Pusey M F, Barrett J and Rudolph T 2012 *Nat. Phys.* **8**, 475
[21] Barnett S 2009 *Quantum Information*, Oxford University Press, pp 103-104
[22] Bandyopadhyay S, Jain R, Oppenheim J and Perry C 2013 preprint *arXiv*:1306.4683
[23] Holevo A S 1973 *J. Multivar. Anal.* **3** 337
[24] Yuen H P, Kennedy R S and Lax M 1975 *IEEE Trans. Inform. Theory* **IT-21** 125
[25] Fuchs C A and van de Graaf J 1999 *IEEE Trans. Inform. Theory* **45** 1216
[26] Bennett C H, Mor T and Smolin J A 1996 *Phys. Rev. A* **54** 2675